

11/14/00
jc952 U.S. PTO

11-16-00

A

PATENT APPLICATION
Express Mail Label No. EL436467966US
Attorney Docket No. NA00-08801

jc490 U.S. PTO
09/7/13095
11/14/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT
APPLICATION TRANSMITTAL LETTER

Asst. Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

Sir:

Enclosed for filing is an ☒ original patent application or, ☐ a continuation-in-part patent application, by inventor(s) Paul F. Hanchett, entitled METHOD AND APPARATUS FOR ESTABLISHING SECURITY SCANNER PARAMETERS IN A COMPUTING SYSTEM.

No. of pages in Application: 17; No. of Claims: 24.

No. of Sheets of Drawings: Formal: 4, Informal: 0.

Also enclosed are:

- ☐ a claim for foreign priority under 35 U.S.C. §§ 119 and/or 365 in
- ☐ a separate document ☐ the declaration;
- ☐ a certified copy of the priority document;
- ☐ an Associate Power of Attorney;
- ☐ ___ verified statement(s) claiming small entity status;
- ☒ a Combined Declaration and Power of Attorney of the inventor(s);
- ☐ a signed Combined Declaration and Power of Attorney of the inventors will follow;
- ☒ an Assignment document and form PTO-1595;
- ☐ a Power of Attorney by Assignee; and
- ☐ Information Disclosure Statement and Form PTO-1449.

The fee has been calculated as follows:

CLAIMS					
	NO. OF CLAIMS		EXTRA CLAIMS	RATE	FEE
Basic Application Fee					\$710.00
Total Claims	24	MINUS 20 =	4	\$18.00=	\$72.00
Independent Claims	3	MINUS 3 =	0	\$80.00=	\$0.00
If multiple dependent claims are presented, add \$260.00					0
Total Application Fee					\$782.00
If verified statement claiming small entity status is enclosed, subtract 50% of Total Application Fee					
Add Recording Fee of \$40.00 if Assignment document is enclosed					\$40.00
TOTAL APPLICATION FEE DUE					\$822.00

- ☒ A check in the amount of \$ 822.00 is enclosed.
- ☐ Application fee will follow with missing parts.
- ☒ Please deduct any underpayments, credit any overpayments, and charge all required extension of time fees to Deposit Account Number 50-1003.

Please direct all correspondence concerning the above-identified application to the following address:

A. Richard Park
Park & Vaughan LLP
508 Second Street, Suite 201
Davis, CA 95616
(530) 759-1661



Respectfully submitted,

By

A. Richard Park
A. Richard Park
Registration No. 41,241

Date: November 14, 2000

PATENT APPLICATION
ATTORNEY DOCKET NO. NA00-08801

5

10

**METHOD AND APPARATUS FOR
ESTABLISHING SECURITY SCANNER
ATTRIBUTES IN A COMPUTER SYSTEM**

15

Inventor: Paul F. Hanchett

BACKGROUND

Field of the Invention

20

The present invention relates to computer security and detection of malicious software. More specifically, the present invention relates to a method and an apparatus for assigning a list of security scanner attributes for computing devices within a hierarchy of computing nodes.

25

Related Art

30

Many computer users, particularly on the Internet, find delight in infecting another user's computer with malicious software, such as a computer virus. A computer virus is designed to replicate itself across a network of computer systems, and to interfere with the normal use of computer systems by possibly denying access, deleting data, or any of a number of other malevolent tricks. As

computer systems become increasingly interconnected, protection from malicious users is becoming increasingly more important.

A software scanner can be used to protect a computer user from malicious software. A scanner makes use of a list of attributes, generated by a computer system administrator, to inspect files and to take actions specified by the list of attributes when it finds any malicious software.

Managing such a list of attributes for virus protection on a large computer network, a Corporate Intranet for example, is difficult because there are many computers and, possibly, many sites separated by large distances. To ensure that the list of attributes provides meaningful protection, the attributes are often managed globally for the network. In order to do so, a security administrator must visit each node in the hierarchy of computing nodes, either in person or across the network, to establish attributes for a software scanner located on each node.

However, a specific node may require a customized list of attributes in order to accommodate a specific hardware configuration or specific functionality.

When a custom list of attributes is used for a specific computing device, the security administrator must remember to reset the custom settings at the node whenever the general list of attributes is changed. This can be a time-consuming task if many nodes in the network must be customized.

What is needed is a system that facilitates both efficient global and local control of a list of scanner attributes throughout a network of computing nodes.

SUMMARY

One embodiment of the present invention provides a system that establishes a list of security scanner attributes for a computing node within a hierarchy of computing nodes. The list of security scanner attributes is associated with a security scanner action to be performed by a security scanner program. The

system establishes a hierarchy of lists of attributes, with each attribute being comprised of an attribute identifier and an attribute value. The attribute value may be either a list of attributes or a controlling value used by the security scanner program to control the operation of the security scanner program. The list of attributes also has a grouping attribute which indicates: that an element of the list may be updated without also updating other elements in the list; that updating an element requires all other elements of the list to be updated; or that updating the element requires the element, all other elements, and all subordinate elements of the list of attributes to be updated.

10 In one embodiment of the present invention, the list of attributes contains an identifier that uniquely identifies the element and a value, wherein the value may itself be a list of elements.

15 In one embodiment of the present invention, the grouping attribute indicates that: the element may be updated without also updating other elements in the list of attributes, updating the element requires all other elements in the list of attributes to be updated, or updating the element requires all other elements in the list of attributes and all subordinate elements in the list of attributes to be updated.

20 In one embodiment of the present invention, updating the element involves overwriting the value with another value, which may be identical to an original value.

In one embodiment of the present invention, updating the element and all other elements of the list of attributes involves overwriting each value with another value, which may be identical to an original value.

25 In one embodiment of the present invention, updating the element, all other elements in the list of attributes, and all subordinate elements of the list of attributes involves overwriting each value with another value, which may be

identical to an original value for each element and each subordinate element of the list of attributes.

In one embodiment of the present invention, if the attribute being updated is itself another list of attributes, the grouping attribute can indicate one of: the attribute can be updated, the content of the list of attributes can be replaced, or the other list of attributes can be merged with the list of attributes

In one embodiment of the present invention, the security scanner program performs a scanning process on files associated with the computing node for malicious computer instructions. Details of the scanning process are specified by the list of security scanner attributes.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 illustrates a hierarchy of computing nodes in accordance with an embodiment of the present invention.

FIG. 2 illustrates the configuration of a single computing node within the hierarchy of computing nodes in accordance with an embodiment of the present invention.

FIG. 3 illustrates a list of security scanner attributes in accordance with an embodiment of the present invention.

FIG. 4 is a flowchart illustrating the processes of establishing a list of security scanner attributes in accordance with an embodiment of the present invention.

FIG. 5 is a flowchart illustrating the process of scanning files in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

The following description is presented to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed
5 embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other embodiments and applications without departing from the spirit and scope of the present invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features
10 disclosed herein.

The data structures and code described in this detailed description are typically stored on a computer readable storage medium, which may be any device or medium that can store code and/or data for use by a computer system. This includes, but is not limited to, magnetic and optical storage devices such as disk
15 drives, magnetic tape, CDs (compact discs) and DVDs (digital versatile discs or digital video discs), and computer instruction signals embodied in a transmission medium (with or without a carrier wave upon which the signals are modulated). For example, the transmission medium may include a communications network, such as the Internet.

20

Computer Systems

FIG. 1 illustrates a hierarchy of computing nodes. Within this hierarchy, computing node 100 is a parent node and is coupled to a number of subordinate child nodes including computing nodes 102, 104, and 106. In addition to being a
25 child node of computing node 100, computing node 104 is itself a parent node for computing nodes 108, 110, and 112. In general, any computing node in the hierarchical network can have a parent node and zero or more child nodes. Note

that computing nodes 100, 102, 104, 106, 108, 110, and 112 may include any type of computer system, including, but not limited to, a computer system based on a microprocessor, a mainframe computer, a digital signal processor, a personal organizer, a device controller, and a computational engine within an appliance.

5 Also note that computing nodes 100, 102, 104, 106, 108, 110, and 112 may be coupled together by any mechanism for communicating across the network, including, but not limited to, a local area network, a wide area network, or a combination of networks.

10 **A representative computing node**

FIG. 2 illustrates the configuration of a single computing node within the hierarchy of computing nodes in accordance with an embodiment of the present invention. Computing node 104 contains a list of security scanner attributes 204 that is used by security scanner program 202 to scan file 212 located on storage
15 device 210 for malicious code. Computing node 104 inherits list of security scanner attributes 204 from its parent node using security scanner establishment mechanism 206. If computing node 104 does not have a parent node, a security administrator 208 can establish list of security scanner attributes 204 by using security parameter establishment mechanism 206.

20 Security administrator 208 uses security parameter establishment mechanism 206 to traverse the list of security scanner attributes 204 to determine if the elements of list of security scanner attributes 204 are allowed to be changed by computing node 104. Details of list of security scanner attributes 204 are provided with the discussion of FIG. 3 below. If allowed, security administrator
25 208 uses security parameter establishment mechanism 206 to establish a changed list of security scanner attributes 204. Security administrator 208 also uses security parameter establishment mechanism 206 to set a grouping attribute at

each node to indicate to child nodes how list of security scanner attributes 204 may be changed.

The list of security scanner attributes

5 FIG. 3 illustrates an example list of security scanner attributes 204. List of security scanner attributes 204 includes attributes 302, 308, 314, 320, and 326. List of security scanner attributes 204 also includes grouping attribute 332. Each attribute includes an attribute identifier and one of: a controlling value and a list of attributes. Attributes 302, 308, 314, 320, and 326 include attribute identifiers 304,
10 310, 316, 322, and 328 respectively. Attributes 302, 314, and 326 include controlling values 306, 318, and 330 respectively while attributes 308 and 320 include list of attributes 312 and 324 respectively.

 List of attributes 312 includes attributes 334 and 340 and grouping attribute 346. Attributes 334 and 340 include attribute identifiers 336 and 342
15 respectively. Attribute 334 includes controlling value 338 while attribute 340 includes list of attributes 344.

 List of attributes 324 includes attributes 348 and 354 and grouping attribute 360. Attributes 348 and 354 include attribute identifiers 350 and 356
20 respectively. Attributes 348 and 354 also include controlling values 352 and 358 respectively.

 List of attributes 344 includes attributes 362 and 368 and grouping attribute 374. Attributes 362 and 368 include attribute identifiers 364 and 370
25 respectively. Attributes 362 and 368 also include controlling values 366 and 372 respectively.

 Grouping attribute 332 indicates to security parameter establishment mechanism 206 how the attributes of list of security scanner attributes 204 may be changed. Grouping attribute 332 indicates one of: each attribute may be changed

individually, all attributes must be changed as a group, and all attributes and subordinate attributes must be changed as a group. Similarly, grouping attributes 346, 360, and 374 indicate how lists of attributes 312, 324, and 344 respectively may be changed.

- 5 Security scanner program 202 uses controlling values 306, 318, 330, 338, 352, 358, and 372 to scan file 212.

Process of establishing a list of security scanner attributes

- 10 FIG. 4 is a flowchart illustrating the process of establishing a list of security scanner attributes, say list of attributes 312. The system starts when security administrator 208 uses security parameter establishment mechanism 206 to initiate changes to list of attributes 312. Security parameter establishment mechanism 206 inspects grouping attribute 346 to determine whether: each element may be changed individually; all elements must be changed as a group; or
15 all elements and subordinate elements must be changed as a group (step 402).

- If all elements and subordinate elements must be changed as a group (step 402), security administrator 208 establishes new values for attributes 362 and 368 in list of attributes 344 (step 404). After updating the attributes in step 404, or if step 402 indicates that updating an element requires all other elements to be
20 updated, security administrator 208 establishes new values for attributes 338 and 344 in list of attributes 312 (step 406).

- After updating the attributes in step 406, or if step 402 indicates that updating an element does not require another element to be updated, security administrator 208 may establish new values for attributes 338 and 344 in list of
25 attributes 312 as desired (step 408).

Process of scanning files for malicious program instructions

FIG. 5 is a flowchart illustrating the process of scanning files in accordance with an embodiment of the present invention. The process starts when security scanner program 202 is activated. Security scanner program 202 determines what files are to be scanned by accessing list of security scanner attributes 204 (step 502). For each file to be scanned, security scanner program 202 scans the file to determine if the file has been infected with malicious code (step 504). If the file has been infected (step 506), security scanner program takes a corrective action specified by list of security scanner attributes 204 (step 508). After step 508, or if the file has not been infected in step 506, security scanner program 202 determines if all specified files have been scanned which means the scan is complete (step 510). If the scan is not complete (step 510), security scanner program 202 returns to scan the next file (step 504). After the scan of all files has been completed, the process ends (step 510).

The foregoing descriptions of embodiments of the invention have been presented for purposes of illustration and description only. They are not intended to be exhaustive or to limit the present invention to the forms disclosed. Accordingly, many modifications and variations will be apparent to practitioners skilled in the art. Additionally, the above disclosure is not intended to limit the present invention. The scope of the present invention is defined by the appended claims.

What Is Claimed Is:

- 1 1. A method for establishing a list of security scanner attributes for a
2 computing node within a hierarchy of computing nodes, the list of security
3 scanner attributes being associated with a security scanner action to be performed
4 by a security scanner program, the method comprising:
5 establishing a hierarchy of lists of attributes, an attribute being comprised
6 of an attribute identifier and an attribute value, the attribute value being comprised
7 of either a list of attributes or a controlling value used by the security scanner
8 program to control an operation of the security scanner program, the list of
9 attributes being comprised of a grouping attribute and a series of one or more
10 attributes;
11 examining the grouping attribute associated with the list of attributes;
12 updating an element of the list of attributes if the grouping attribute
13 indicates that the element may be updated without also updating other elements in
14 the list of attributes;
15 updating the element and all other elements of the list of attributes if the
16 grouping attribute indicates that updating the element requires all other elements
17 to be updated; and
18 updating the element, all other elements, and all subordinate elements of
19 the list of attributes if the grouping attribute indicates that updating the element
20 requires all subordinate elements of the list of attributes to be updated.
- 1 2. The method of claim 1, wherein the element of the list of attributes
2 contains an identifier that uniquely identifies the element and a value, wherein the
3 value may itself be a list of elements.

1 3. The method of claim 1, wherein the grouping attribute indicates
2 one of:
3 the element may be updated without also updating other elements in the
4 list of attributes;
5 updating the element requires all other elements in the list of attributes to
6 be updated; and
7 updating the element requires all other elements in the list of attributes and
8 all subordinate elements in the list of attributes to be updated.

1 4. The method of claim 2, wherein updating the element involves
2 overwriting the value with another value that may be identical to an original
3 value.

1 5. The method of claim 2, wherein updating the element and all other
2 elements of the list of attributes involves overwriting each value with another
3 value that may be identical to an original value.

1 6. The method of claim 2, wherein updating the element, all other
2 elements in the list of attributes, and all subordinate elements of the list of
3 attributes involves overwriting each value with another value that may be identical
4 to an original value for each element and each subordinate element of the list of
5 attributes.

1 7. The method of claim 2, wherein if the attribute being updated is
2 itself another list of attributes, the grouping attribute can indicate one of:
3 the attribute can be updated;
4 a content of the list of attributes can be replaced; and

5 the other list of attributes can be merged with the list of attributes.

1 8. The method of claim 1, wherein the security scanner program
2 performs a scanning process on files associated with the computing node for
3 malicious computer instructions, wherein details of the scanning process are
4 specified by the list of security scanner attributes.

1 9. A computer-readable storage medium storing instructions that
2 when executed by a computer causes the computer to perform a method for
3 establishing a list of security scanner attributes for a computing node within a
4 hierarchy of computing nodes, the list of security scanner attributes being
5 associated with a security scanner action to be performed by a security scanner
6 program, the method comprising:
7 establishing a hierarchy of lists of attributes, an attribute being comprised
8 of an attribute identifier and an attribute value, the attribute value being comprised
9 of either a list of attributes or a controlling value used by the security scanner
10 program to control an operation of the security scanner program, the list of
11 attributes being comprised of a grouping attribute and a series of one or more
12 attributes;
13 examining the grouping attribute associated with the list of attributes;
14 updating an element of the list of attributes if the grouping attribute
15 indicates that the element may be updated without also updating other elements in
16 the list of attributes;
17 updating the element and all other elements of the list of attributes if the
18 grouping attribute indicates that updating the element requires all other elements
19 to be updated; and
20 updating the element, all other elements, and all subordinate elements of

21 the list of attributes if the grouping attribute indicates that updating the element
22 requires all subordinate elements of the list of attributes to be updated.

1 10. The computer-readable storage medium of claim 9, wherein the
2 element of the list of attributes contains an identifier that uniquely identifies the
3 element and a value, wherein the value may itself be a list of elements.

1 11. The computer-readable storage medium of claim 9, wherein the
2 grouping attribute indicates one of:
3 the element may be updated without also updating other elements in the
4 list of attributes;
5 updating the element requires all other elements in the list of attributes to
6 be updated; and
7 updating the element requires all other elements in the list of attributes and
8 all subordinate elements in the list of attributes to be updated.

1 12. The computer-readable storage medium of claim 10, wherein
2 updating the element involves overwriting the value with another value that may
3 be identical to an original value.

1 13. The computer-readable storage medium of claim 10, wherein
2 updating the element and all other elements of the list of attributes involves
3 overwriting each value with another value that may be identical to an original
4 value.

1 14. The computer-readable storage medium of claim 10, wherein
2 updating the element, all other elements in the list of attributes, and all

3 subordinate elements of the list of attributes involves overwriting each value with
4 another value that may be identical to an original value for each element and each
5 subordinate element of the list of attributes.

1 15. The computer-readable storage medium of claim 10, wherein if the
2 attribute being updated is itself another list of attributes, the grouping attribute can
3 indicate one of:

4 the attribute can be updated;
5 a content of the list of attributes can be replaced; and
6 the other list of attributes can be merged with the list of attributes.

1 16. The computer-readable storage medium of claim 9, wherein the
2 security scanner program performs a scanning process on files associated with the
3 computing node for malicious computer instructions, wherein details of the
4 scanning process are specified by the list of security scanner attributes.

1 17. An apparatus that facilitates establishing a list of security scanner
2 attributes for a computing node within a hierarchy of computing nodes, the list of
3 security scanner attributes being associated with a security scanner action to be
4 performed by a security scanner program, comprising:
5 an establishing mechanism that is configured to establish a hierarchy of
6 lists of attributes, an attribute being comprised of an attribute identifier and an
7 attribute value, the attribute value being comprised of either a list of attributes or a
8 controlling value used by the security scanner program to control an operation of
9 the security scanner program, the list of attributes being comprised of a grouping
10 attribute and a series of one or more attributes;
11 an examining mechanism that is configured to examine the grouping

12 attribute associated with the list of attributes;
13 an updating mechanism that is configured to update an element of the list
14 of attributes if the grouping attribute indicates that the element may be updated
15 without also updating other elements in the list of attributes;
16 wherein the updating mechanism is further configured to update the
17 element and all other elements of the list of attributes if the grouping attribute
18 indicates that updating the element requires all other elements to be updated; and
19 wherein the updating mechanism is further configured to update the
20 element, all other elements, and all subordinate elements of the list of attributes if
21 the grouping attribute indicates that updating the element requires all subordinate
22 elements of the list of attributes to be updated.

1 18. The apparatus of claim 17, wherein the element of the list of
2 attributes contains an identifier that uniquely identifies the element and a value,
3 wherein the value may itself be a list of elements.

1 19. The apparatus of claim 17, wherein the grouping attribute indicates
2 one of:
3 the element may be updated without also updating other elements in the
4 list of attributes;
5 updating the element requires all other elements in the list of attributes to
6 be updated; and
7 updating the element requires all other elements in the list of attributes and
8 all subordinate elements in the list of attributes to be updated.

1 20. The apparatus of claim 18, wherein the updating mechanism is
2 configured to overwrite the value with another value that may be identical to an

1 original value.

1 21. The apparatus of claim 18, wherein the updating mechanism is
2 configured to update the element and all other elements of the list of attributes by
3 overwriting each value with another value that may be identical to an original
4 value.

1 22. The apparatus of claim 18, wherein the updating mechanism is
2 configured to update the element, all other elements in the list of attributes, and all
3 subordinate elements of the list of attributes by overwriting each value with
4 another value that may be identical to an original value for each element and each
5 subordinate element of the list of attributes.

1 23. The apparatus of claim 18, wherein if the attribute being updated is
2 itself another list of attributes, the grouping attribute can indicate one of:
3 the attribute can be updated;
4 a content of the list of attributes can be replaced; and
5 the other list of attributes can be merged with the list of attributes.

1 24. The apparatus of claim 17, wherein the security scanner program is
2 configured to perform a scanning process on files associated with the computing
3 node for malicious computer instructions, wherein details of the scanning process
4 are specified by the list of security scanner attributes.

METHOD AND APPARATUS FOR ESTABLISHING SECURITY SCANNER ATTRIBUTES IN A COMPUTER SYSTEM

ABSTRACT

One embodiment of the present invention provides a system that establishes a list of security scanner attributes for a computing node within a hierarchy of computing nodes. The list of security scanner attributes is associated with a security scanner action to be performed by a security scanner program. The system establishes a hierarchy of lists of attributes, with each attribute being comprised of an attribute identifier and an attribute value. The attribute value may be either a list of attributes or a controlling value used by the security scanner program to control the operation of the security scanner program. The list of attributes also has a grouping attribute which indicates: that an element of the list may be updated without also updating other elements in the list; that updating an element requires all other elements of the list to be updated; or that updating the element requires the element, all other elements, and all subordinate elements of the list of attributes to be updated.

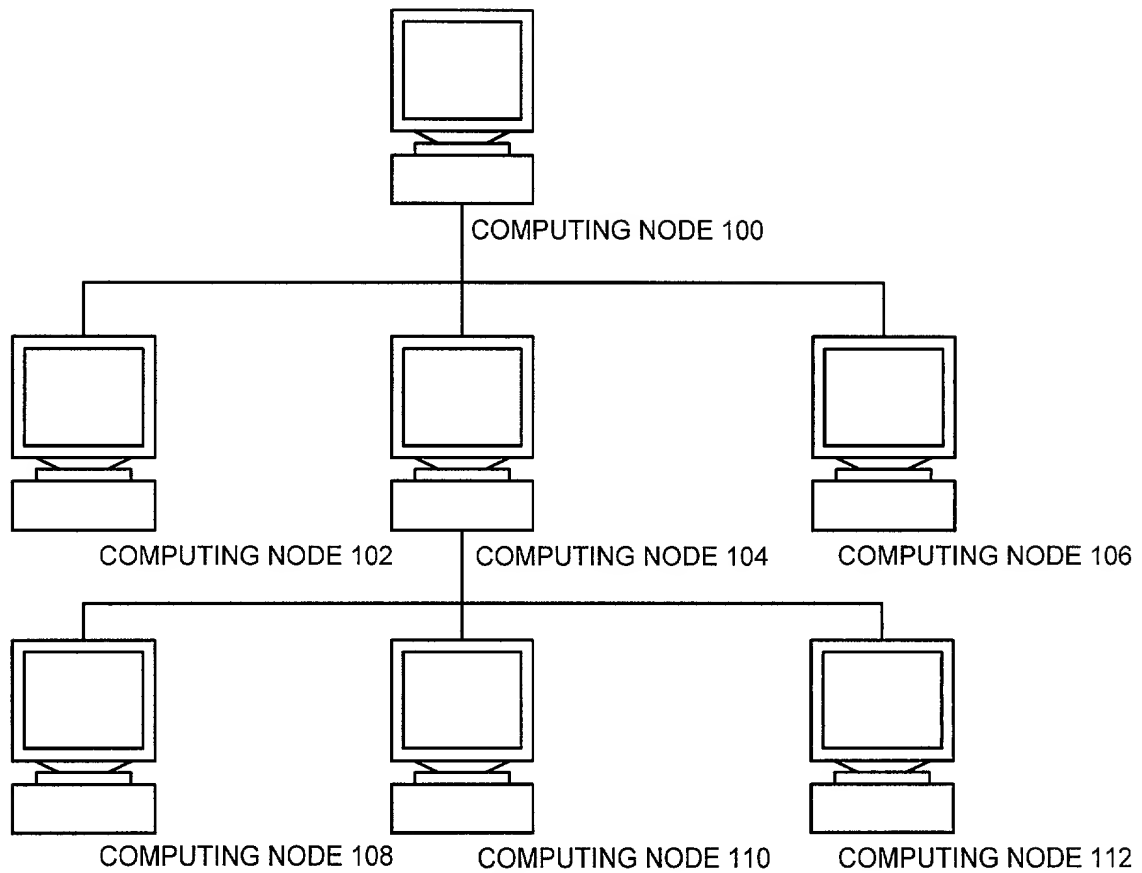


FIG. 1

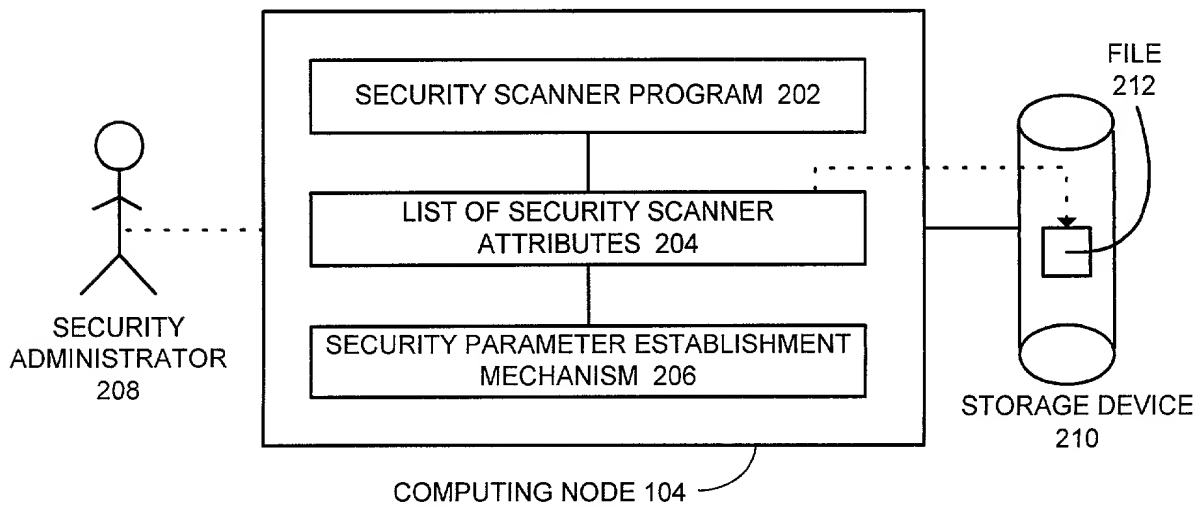
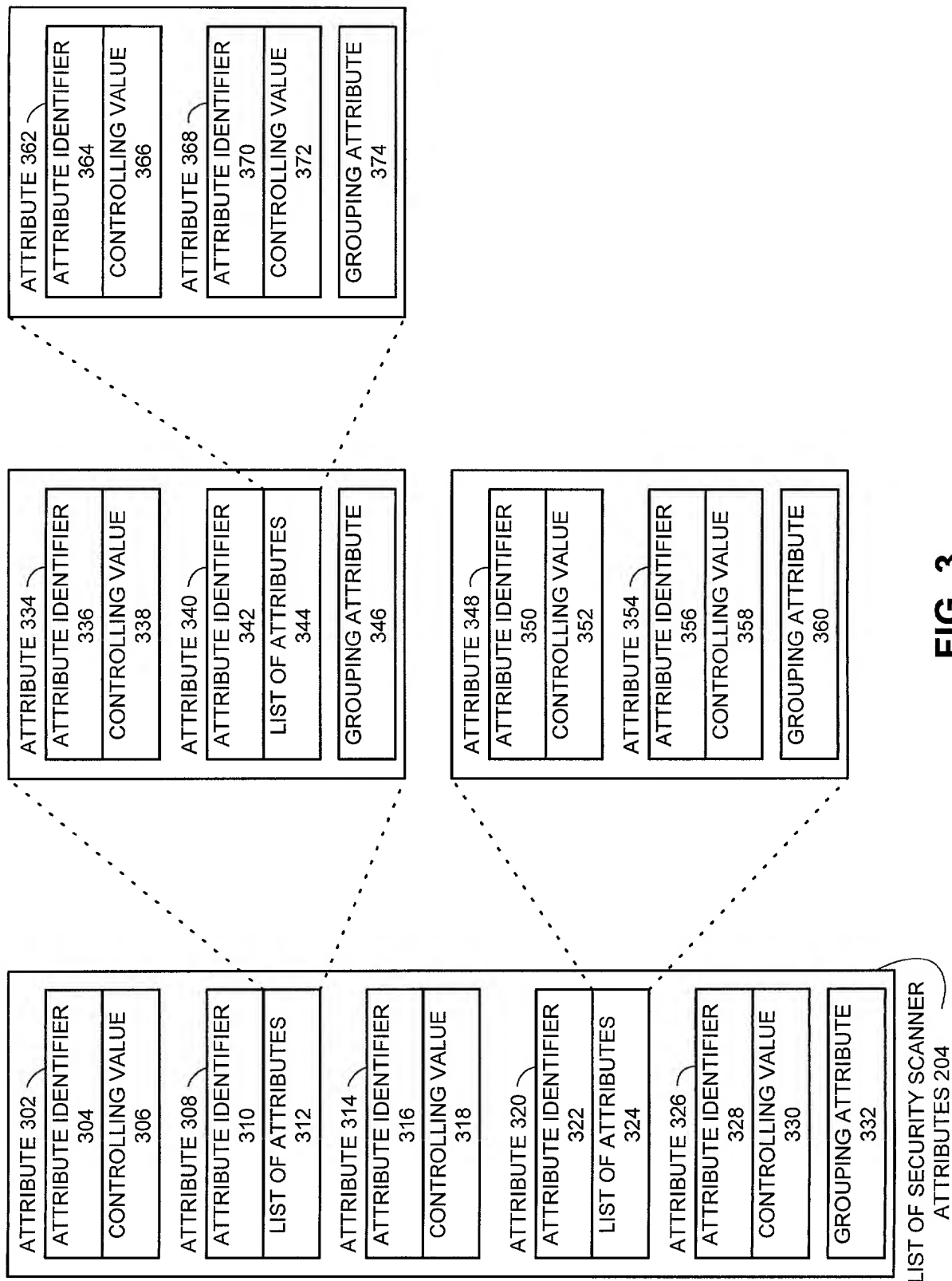


FIG. 2



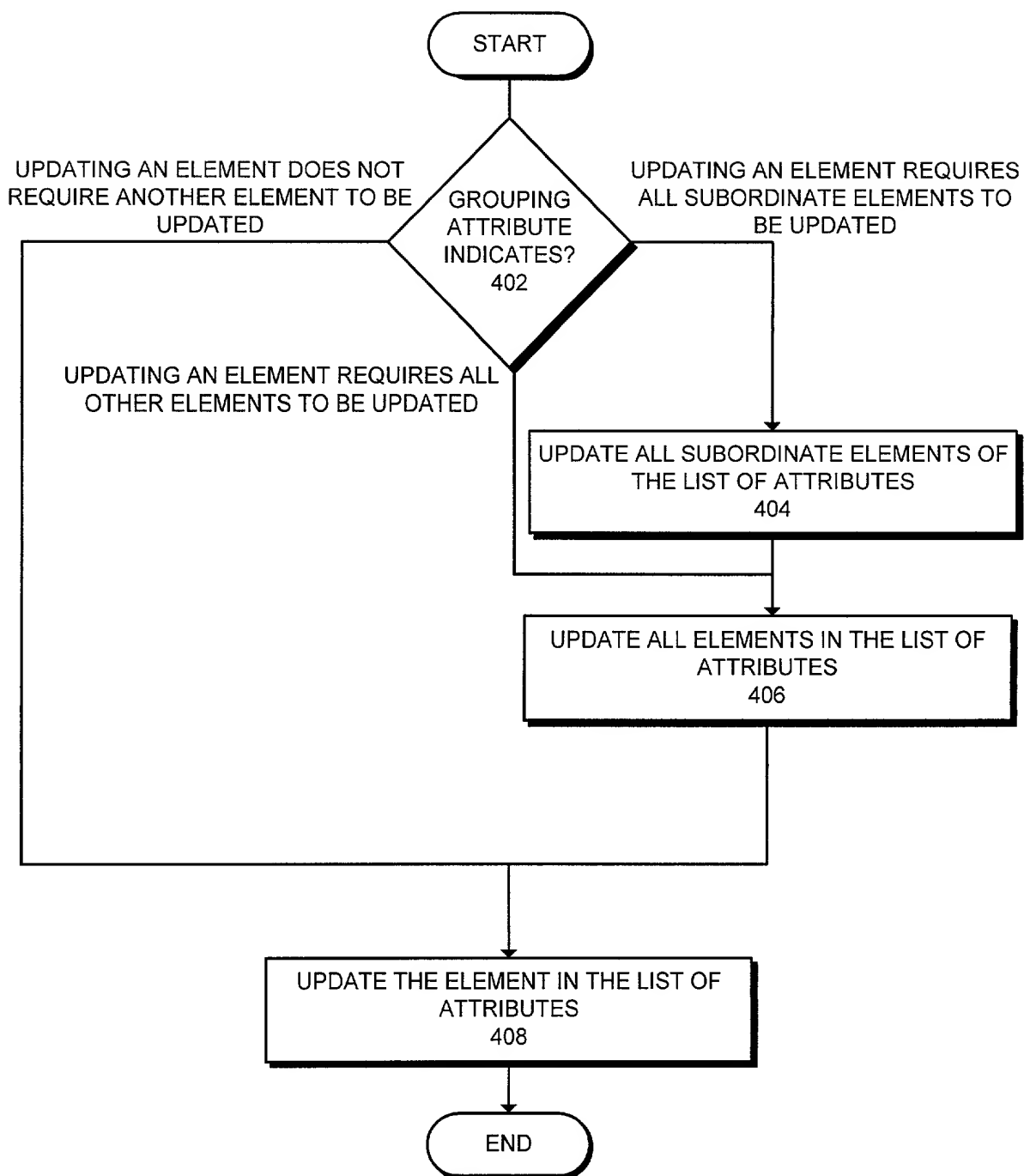


FIG. 4

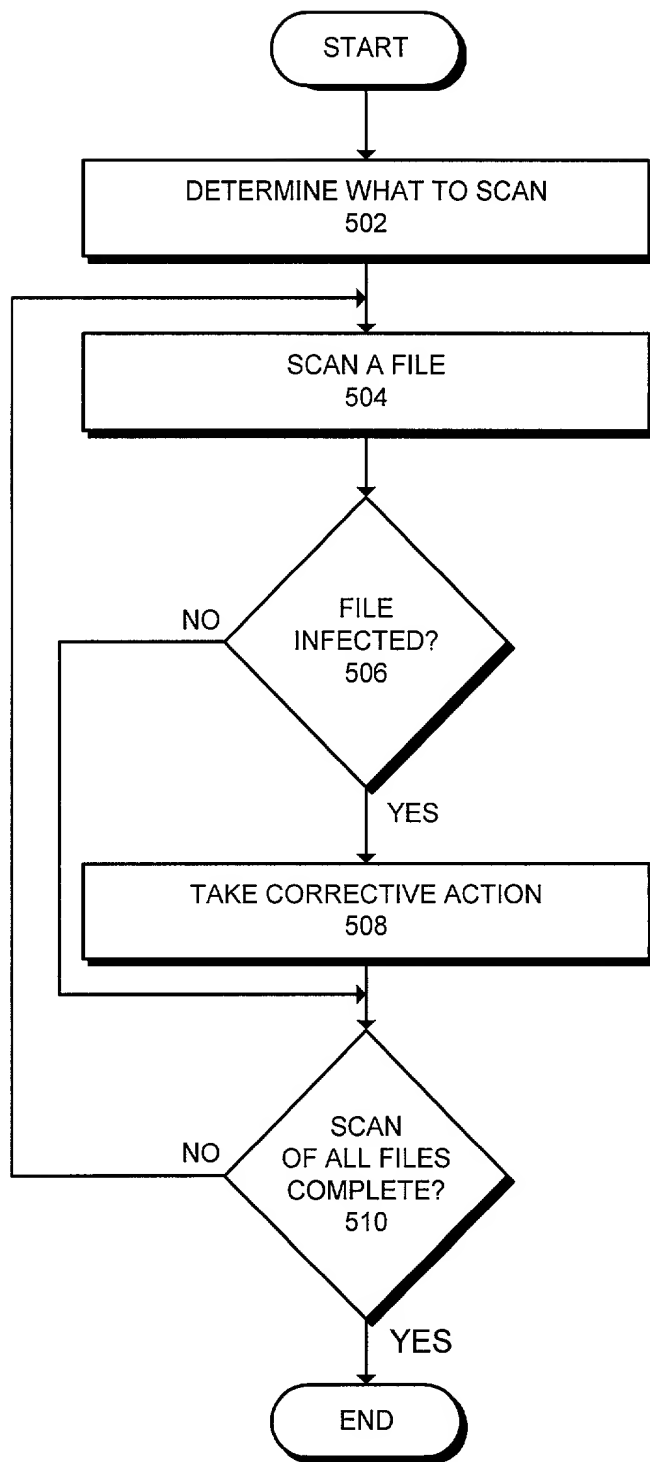


FIG. 5

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below-named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below by my name;

I believe I am the original, first and sole inventor, if only one name is listed below, or an original, first and joint inventor if multiple names are listed below, of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND APPARATUS FOR ESTABLISHING SECURITY SCANNER PARAMETERS IN A COMPUTING SYSTEM

for which a patent application:

☒ is attached hereto.

☐ was filed in the United States on _ as Application No. _;

☐ with amendment(s) filed on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the application identified above, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information known to me to be material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56, which states in relevant part:

Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section.... The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office....

I hereby claim foreign priority benefits under Title 35, United States Code, §119(a)-(d), of any foreign application(s) for patent or inventor's certificate as indicated below and have also identified below any foreign application for patent or inventor's certificate on this invention having a filing date before that of the application on which priority is claimed:

EARLIEST FOREIGN APPLICATION(S), IF ANY, FILED PRIOR TO THE FILING DATE OF THE APPLICATION			
APPLICATION NUMBER	COUNTRY	DATE OF FILING (Day, Month, Year)	PRIORITY CLAIMED
			YES <input type="checkbox"/> NO <input type="checkbox"/>

I hereby claim the benefit under Title 35, United States Code, §119(e), of any United States provisional application(s) listed below:

APPLICATION NUMBER	DATE OF FILING

I hereby claim the benefit under Title 35, United States Code, §120, of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose information that is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION NUMBER	DATE OF FILING	STATUS		
		PATENTED	PENDING	ABANDONED

I hereby appoint Daniel E. Vaughan (Reg. No. 42,199) and A. Richard Park (Reg. No. 41,241) to prosecute this application

and transact all business in the Patent and Trademark Office connected therewith, and to file, prosecute and transact all business in connection with international applications directed to said invention.

Address correspondence to:
Park & Vaughan LLP
508 Second Street, Suite 201
Davis, CA 95616



22835

PATENT TRADEMARK OFFICE

Direct telephone calls to:
 A. Richard Park
 (530) 759-1661

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the same so made are punishable by fine or imprisonment, or both, under Title 18, United States Code, §1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

	Name and Citizenship	Paul F. Hanchett	United States of America
	Residence Address	555 SW Viewcrest Drive, Gresham, OR 97080	
	Postal Address (if different from Residence)		
	Signature and Date	<i>Paul F. Hanchett</i>	Date <i>Oct. 7, 2000</i>
	Name and Citizenship		
	Residence Address		
	Postal Address (if different from Residence)		
	Signature and Date		Date
3	Name and Citizenship		
	Residence Address		
	Postal Address (if different from Residence)		
	Signature and Date		Date
4	Name and Citizenship		
	Residence Address		
	Postal Address (if different from Residence)		
	Signature and Date		Date
5	Name and Citizenship		
	Residence Address		
	Postal Address (if different from Residence)		
	Signature and Date		Date

Additional inventor name(s) and signature(s) attached?: YES ☐ NO ☒